EXHIBIT 9

Trials@uspto.gov
Tel: 571-272-7822

Paper 19
Entered: March 23, 2018

UNITED STATES PATENT AND TRADEMARK OFFICE

BEFORE THE PATENT TRIAL AND APPEAL BOARD

UNIFIED PATENTS INC.,
Petitioner,

v.

TEXTILE COMPUTER SYSTEMS, INC.,
Patent Owner.

Case IPR2017-00296
Patent 8,505,079 B2

Before JUSTIN T. ARBES, STACEY G. WHITE, and SCOTT B. HOWARD, *Administrative Patent Judges*.

HOWARD, *Administrative Patent Judge*.

FINAL WRITTEN DECISION
35 U.S.C. § 318(a) and 37 C.F.R. § 42.73

I. INTRODUCTION

Unified Patents Inc. ("Petitioner") filed a Petition (Paper 2, "Pet.") to institute an *inter partes* review of claims 1, 3, 6–9, 11, 13, and 16–19 of U.S. Patent No. 8,505,079 B2 (Ex. 1001, "the '079 patent") pursuant to 35 U.S.C. §§ 311–19. Textile Computer Systems, Inc. ("Patent Owner") filed a Patent Owner Preliminary Response. Paper 8 ("Prelim. Resp."). We instituted an *inter partes* review of claims 1, 3, 6–9, 11, 13, and 16–19 on certain grounds of unpatentability alleged in the Petition (Paper 9, "Dec.").

After institution of trial, Patent Owner filed a Patent Owner Response (Paper 13, "PO Resp."). Petitioner filed a Reply (Paper 17, "Reply"). Neither Patent Owner nor Petitioner requested an oral hearing. *See* Paper 18.

The Board has jurisdiction under 35 U.S.C. § 6(b). This Final Written Decision is entered pursuant to 35 U.S.C. § 318(a) as to the patentability of the claims for which we instituted trial. For the reasons that follow, we conclude that Petitioner has not demonstrated by a preponderance of the evidence that claims 1, 3, 6–9, 11, 13, and 16–19 of the '079 patent are unpatentable.

II. BACKGROUND

A. Related Proceedings

The parties identify the following former proceedings[1] involving the '079 patent: *Textile Comp. Sys., Inc. v. Fort Worth City Credit Union,* No. 2:16-cv-01048 (E.D. Tex.); *Textile Comp. Sys., Inc. v. Sabine Fed. Credit Union*, No. 2:16-cv-01047 (E.D. Tex.); and *Textile Comp. Sys., Inc. v.*

[1] We take notice that all of the cases have settled.

E. Tex. Prof'l Credit Union, No. 2:16-cv-00702 (E.D. Tex.). Pet. 73; Paper 4, 1.

B. The '079 Patent

The '079 patent "relates to security protocols for use in securing and/or restricting access to personal other confidential information, physical locations and the like." Ex. 1001, 1:6–8. According to the '079 patent, the protection of personal information "is of ever increasing concern" and has led to the use of "various security protocols employed for the protection of such resources," which "almost universally include[] some means for authenticating the identity of a person, entity, device or the like attempting to gain access to a secured resource." *Id.* at 1:16–28. However, "a security breach in connection with a single secured resource may jeopardize the security of all other secured resources." *Id.* at 1:42–44.

The '079 patent is directed to improving "the prior art by providing a system and related method by which authentication may be more securely conducted." *Id.* at 1:45–49. The '079 patent provides "a system and related method that is robust in specific implementation and readily usable" and "is economical in implementation and therefore readily accessible to virtually any application." *Id.* at 1:49–56.

The invention disclosed in the '079 patent is a transaction protocol between three parties—the end user (for example, a purchaser of an item), a service client (for example, a seller of goods or services), and a service provider (for example, a credit card processor)—that is conducted with six messaging steps. *See*, *e.g.*, *id*. at Figs. 1, 4, 1:60–2:7, 2:27–38, 4:15–47, 7:14–8:3. Figure 4 of the '079 patent, as annotated by Petitioner (Pet. 3), is shown below:

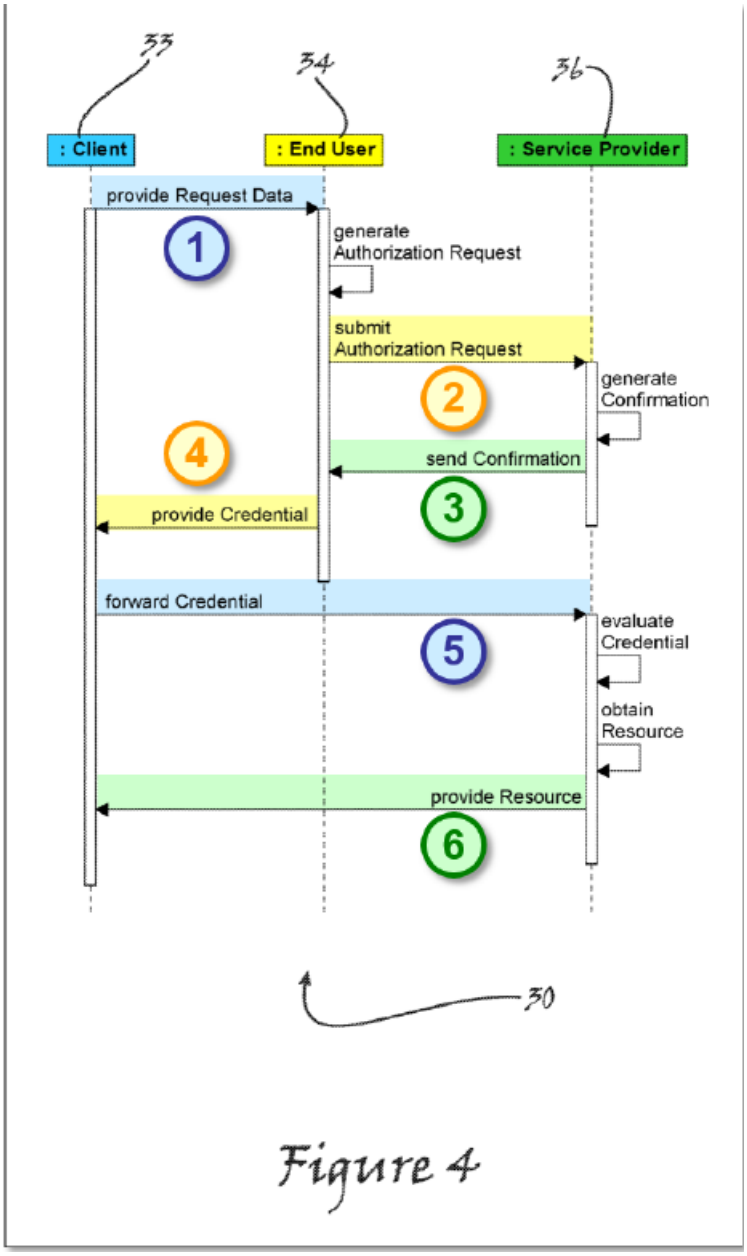

Figure 4

Figure 4 shows "various interactions [that] generally take place during the operation of the authentication system and method of the present invention" (Ex. 1001, 3:15–17) in which the six different messaging steps are color coded based on the sender—blue for the service client, yellow for the end user, and green for the service provider (*see* Pet. 2–4).

First, the service client sends data that will be used to generate a request to the end user. Ex. 1001, Fig. 4, 5:35–45. Second, the end user sends a request based on the received data to the service provider. *Id.* at Fig. 4, 5:45–49. Once the service provider receives the message, it "determines whether the end user 34 making the request is authorized or otherwise permitted to make use of the authentication system 30." *Id*. at 5:50–54; *see also id.* at 13:34–53. The system will continue only if the service provider authenticates the identity of the end user; otherwise, it will terminate. *Id.* at 5:54–60, 13:34–53. The '079 patent states that a critical aspect of the present invention is preventing the service client from having access to the common identifier of the secured resource that can be used to gain access to the secured resource without again gaining authorization from the end user:

> *In a critical aspect* of the authentication system 30 and method 46 *of the present invention*, an additional security measure is implemented by requiring that the service client 33 be restricted from access to the common identifier for the secured resource, e.g. the account number for a credit card or financial deposit account; the Social Security Number of a patient; the account number of an ATM card; or the like. . . .
>
> *In accordance with a critical aspect of the present invention*, however, the automobile fueling station, restaurant or on-line retailer cannot be provided with or otherwise be made aware of either the consumer's credit card or checking account number and also must not be given any information that would allow the automobile fueling station, restaurant or on-line retailer to repeat the transaction without again obtaining authorization from the consumer.

Id. at 8:4–10, 10:29–36 (emphases added); *see also id.* at 7:14–46 (emphasizing the importance of restricting the service client from having full access to the secured resource).

Third, after the service provider determines that the end user is authorized to access a secured resource, the service provider sends a confirmation back to the end user. *Id.* at Fig. 4, 6:12–18. Fourth, the end user sends an authorization credential to the service client, which will allow limited access to the secured resource. *Id.* at Fig. 4, 6:18–21, 6:45–7:3. Fifth, the service client sends a message to the service provider with the authentication credential. *Id.* at Fig. 4, 6:45–7:3. Sixth, after confirming the authentication credential, the service provider sends the service client the secured resource. *Id.* at Fig. 4, 7:4–13, 16:16–40.

C. The Challenged Claims

We instituted trial on claims 1, 3, 6–9, 11, 13, and 16–19. Claims 1 and 11 are independent claims. Claim 1 is illustrative of the challenged claims and is reproduced below:

> 1. An authentication system for authenticating the identity of a requester of access by an unauthorized service client to a secured resource, said authentication system comprising:
>
> a messaging gateway having a first set of instructions embodied in a computer readable medium, said first set of instructions operable to receive from a requester purporting to be an authorized user of a secured resource a request for access by an unauthorized service client to said secured resource;
>
> a server in secure communication with said messaging gateway, said server having a second set of instructions embodied in a computer readable medium operable to determine a key string known to both said secured resource and the authorized user said requestor purports to be, said key string being adapted to provide a basis for authenticating the identity of said requester;
>
> a service user interface in communication with said server, said service user interface having a third set of instructions embodied in a computer readable medium operable to receive input from said unauthorized service client;

> wherein said second set of instructions is further operable to receive an authentication credential from said unauthorized service client associated with said request for access, said authentication credential having been provided to said unauthorized service client by said requestor; and
>
> wherein said second set of instructions is further operable to evaluate said authentication credential to authenticate the identity of said requester.

Id. at 17:28–57.

D. Instituted Grounds of Unpatentability

We instituted *inter partes* review of claim 1, 3, 6–9, 11, 13, and 16–19 of the '079 patent on the following grounds:

References	Basis[2]	Challenged Claims
Johnson[3] and Stambaugh[4]	§ 103(a)	1, 6, 7, 9, 11, 16, 17, and 19
Johnson, Stambaugh, and Sellars[5]	§ 103(a)	3, 8, 13, and 18

In support of its challenge, Petitioner relies on the Declaration of Stephen Craig Mott (Ex. 1007). Patent Owner relies on the Declaration of Richard Oglesby (Ex. 2004).

---

[2] The Leahy-Smith America Invents Act ("AIA") included revisions to 35 U.S.C. § 100 *et seq.* effective on March 16, 2013. Because the '079 patent issued from an application filed before March 16, 2013, we apply the pre-AIA versions of the statutory bases for unpatentability.

[3] U.S. Patent Application Publication No. 2006/0235796 A1 (publ. Oct. 19, 2006) (Ex. 1004, "Johnson").

[4] U.S. Patent No. 7,657,489 B2 (issued Feb. 2, 2010) (Ex. 1005, "Stambaugh").

[5] U.S. Patent Application Publication No. 2006/0173794 A1 (publ. Aug. 3, 2006) (Ex. 1006, "Sellars").

III. ANALYSIS

A. Constitutionality of Inter Partes *Review Proceedings*

As a preliminary matter, Patent Owner argues that *inter partes* review proceedings are unconstitutional. PO Resp. 51–55. As Petitioner points out, however, and as Patent Owner admits, "current binding Federal Circuit precedent holds that *inter partes* reviews are not unconstitutional." Reply 26 (citing *MCM Portfolio LLC v. Hewlett-Packard Co.*, 812 F.3d 1284 (Fed. Cir. 2015)); *see* PO Resp. 52.

B. Claim Construction

In an *inter partes* review, claim terms in an unexpired patent are interpreted according to their broadest reasonable construction in light of the specification of the patent in which they appear. 37 C.F.R. § 42.100(b); *Cuozzo Speed Techs., LLC v. Lee*, 136 S. Ct. 2131, 2142–46 (2016). We interpret claim terms using "the broadest reasonable meaning of the words in their ordinary usage as they would be understood by one of ordinary skill in the art, taking into account whatever enlightenment by way of definitions or otherwise that may be afforded by the written description contained in the applicant's specification." *In re Morris*, 127 F.3d 1048, 1054 (Fed. Cir. 1997). "Under a broadest reasonable interpretation, words of the claim must be given their plain meaning, unless such meaning is inconsistent with the specification and prosecution history." *Trivascular, Inc. v. Samuels*, 812 F.3d 1056, 1062 (Fed. Cir. 2016).

There are two exceptions to giving a term its plain meaning: "1) when a patentee sets out a definition and acts as his own lexicographer," and "2) when the patentee disavows the full scope of a claim term either in the specification or during prosecution." *Thorner v. Sony Computer Entm't Am.*

LLC, 669 F.3d 1362, 1365 (Fed. Cir. 2012). In order to act as a lexicographer, a patentee must "clearly set forth a definition of the disputed claim term" and "clearly express an intent to define the term." *Id.*; *see also In re Paulsen*, 30 F.3d 1475, 1480 (Fed. Cir. 1994) (holding that an applicant may act as his own lexicographer by providing a definition of the term in the specification with "reasonable clarity, deliberateness, and precision"). Similarly, disavowal requires that "the specification [or prosecution history] make[ ] clear that the invention does not include a particular feature." *SciMed Life Sys., Inc. v. Advanced Cardiovascular Sys., Inc.*, 242 F.3d 1337, 1341 (Fed. Cir. 2001); *see also In re Abbott Diabetes Care Inc.* 696 F.3d 1142, 1149–50 (Fed. Cir. 2012) (holding that the broadest reasonable interpretation of the claim was limited when the specification "'repeatedly, consistently, and exclusively' depict[ed] an [embodiment] without external cables or wires while simultaneously disparaging sensors with external cables or wires") (quoting *Irdeto Access, Inc. v. Echostar Satellite Corp.*, 383 F.3d 1295, 1303 (Fed. Cir. 2004)).

We need only construe those claim limitations "that are in controversy, and only to the extent necessary to resolve the controversy." *Vivid Techs., Inc. v. Am. Sci. & Eng'g, Inc.*, 200 F.3d 795, 803 (Fed. Cir. 1999)).

Petitioner proposes constructions of three terms: "unauthorized service client," "messaging gateway," and "key string." Pet. 13–16. Patent Owner proposes express constructions for "key string," "secured resource," and "input." PO Resp. 25–33. In our Decision on Institution, we construed the terms "key string," "secured resource," and "input" as follows.

Claim term	Construction
"key string"	Broad enough to encompass an ordered sequence of any subset of symbols selected from a set of symbols wherein each symbol forming the set may be represented in both a format that may be perceived by an end user and a format that may be recognized by software or hardware and is known to both said secured resource and the authorized user said requestor purports to be and adapted to provide a basis for authenticating the identity of said requester.[6] Dec. 8–10
"secured resource"	The claims require the authorized user to control access to the secured resource, but do not require the authorized user to otherwise control the secured resource. Dec. 10–11
"input"	Broad enough to encompass any type of input, including input composed of only the authentication credential. Dec. 11–12

In its Response, Patent Owner argues that we erred in construing those terms. PO Resp. 25–33. For the reasons discussed below, we are persuaded,

[6] In our Decision, we declined to limit the key string to one that does not reveal the common identifier of the secured resource, such as the bank account or credit card number, or any other information that would allow the unauthorized service client to gain access to the secured resource without again obtaining authorization from the authorized user. Dec. 8–10.

with the benefit of the full record before us, to alter our construction of the claim term "key string" as argued by Patent Owner during trial.[7]

1. "Key String"

Petitioner asserts that the broadest reasonable construction of "key string" is broad enough to encompass:

> an ordered sequence of any subset of symbols selected from a set of symbols wherein each symbol forming the set may be represented in both a format that may be perceived by an end user 34 and a format that may be recognized by software or hardware that may be used to provide a basis for authenticating the identity of the requester.

Pet. 16 (citing Ex. 1001, 15:29–36).

Petitioner further argues that Patent Owner's attempt to limit the scope of the claim term is premised on "the claims requir[ing] the 'key string' to be the same as the 'authentication credential.'" Reply 3. According to Petitioner:

> It is well-established that "a particular embodiment appearing in the written description may not be read into a claim when the claim language is broader than the embodiment." *SuperGuide Corp. v. DirectTV Enters., Inc.*, 358 F.3d 870, 875 (Fed Cir. 2004). Therefore, the Board should reject [Patent Owner's] underlying requirement that the "key string" must necessarily be the same as the "authentication credential." Consequently, [Patent Owner's] criticisms of the Board's construction should

[7] As we noted in our Decision, we had not yet "made a final determination as to . . . the construction of any claim term." Dec. 31. Additionally, during trial, Petitioner had the opportunity to—and did in fact—dispute Patent Owner's claim construction arguments and argue how the claims allegedly are unpatentable under Patent Owner's proposed construction. *See*, *e.g.*, Reply 20–21 (Petitioner argues Johnson teaches the input limitation of claims 1 and 11 under Patent Owner's proposed construction).

> be disregarded because they are based on this erroneous requirement.

Reply 4.

Petitioner further argues that there is no need to construe this limitation because "[Patent Owner] does not contend *Johnson's* payment token fails to teach [Patent Owner's] construction of 'key string.'" *Id.*

Patent Owner argues that "[t]he Board's conclusion that the key string can include the primary account number (sensitive data element) is contrary to the specification." PO Resp. 26. Relying on the same portion of the '079 patent as Petitioner, Patent Owner contends a "string" is "an ordered sequence of any subset of symbols selected from a set of symbols wherein each symbol forming the set may be represented in both a format that may be perceived by an end user and a format that may be recognized by software or hardware." *Id.* (citing Ex. 1001, 15:29–41). Additionally, based on various examples in the '079 patent, Patent Owner contends a "key string" must not only provide a basis for authenticating the identity of the end user, but must also restrict access of the common identifier for the secure resource to the service client, such as the merchant:

> The specification also describes the requirements for the content of the key string. In particular, the content of the 'key string' must provide a basis to authenticate the identity of the end user to the service provider and at the same time restrict access to the common identifier for the secured resource to the service client (merchant).

Id. at 26–27 (citing Ex. 1001, 8:4–10). According to Patent Owner, this construction of key string "does not improperly import a limitation of a specific embodiment into the claim but rather reads the term consistently with explicit requirement in the specification regarding the content of the

key string in practicing the invention." *Id.* at 28 (emphasis omitted) (citing Ex. 2004 ¶¶ 49–52).

The '079 patent contains an express definition of the term "string":

> *It is now noted that as used herein a "string" shall for purposes of the present invention be expressly defined to mean* "an ordered sequence of any subset of symbols selected from a set of symbols wherein each symbol forming the set may be represented in both a format that may be perceived by an end user 34 and a format that may be recognized by software or hardware," e.g. the set of all alphabetic and numeric characters in the English language.

Ex. 1001, 15:29–36 (emphasis added). This express definition describes the format of a "string" as that term is used in the '079 patent. It does not describe, however, the content of the claimed "key string" or how it is used. As to those aspects, independent claims 1 and 11 require that the key string be "known to both said secured resource and the authorized user said requestor purports to be" and "adapted to provide a basis for authenticating the identity of said requester." *Id.* at 17:40–42, 18:48–53.

Moreover, based on the complete record, we agree with Patent Owner and Mr. Oglesby that the system (claim 1) and method (claim 11) recited in the claims must prohibit the service client from accessing a common identifier of the secured resource, such as the key string used to authenticate the identity of the end user. *See* PO Resp. 26–28; Ex. 2004 ¶¶ 50–53.

We begin with the words of the claim. The server limitation recited in claim 1 and the determining limitation recited in claim 11 focus on the method and apparatus used by the server to authenticate the identity of the authorized user who is seeking access to the secured resource. Specifically,

the first limitation of claim 1[8] recites a messaging gateway that receives a request from a requester purporting to be the authorized user seeking to allow an unauthorized service client access to a secured resource: "a messaging gateway . . . receiv[ing] from a requester purporting to be an authorized user of a secured resource a request for access by an unauthorized service client to said secured resource." Ex. 1001, 17:31–36.

The claim continues by reciting a server in communication with the messaging gateway that received the request. *Id*. at 17:37–43. The server includes a set of instructions for "determin[ing] a key string known to both [the] secured resource and the authorized user said request[e]r purports to be, [the] key string being adapted to provide a basis for authenticating the identity of [the] requester." *Id.* As discussed in the Specification, this refers to the secured resource (e.g., service provider) determining whether the authorized user is authorized to use the system: "Once a submitted request message 84 is received by the service provider 36, the service provider 36 preferably *determines whether the end user 34 making the request is authorized* or otherwise permitted to make such use of the authentication system 30." *Id*. at 5:50–54 (emphasis added).

According to the portion of the '079 patent cited by Patent Owner (PO Resp. 26–27), preventing the service client, such as a merchant, from having access to the common identifier that is used to authenticate the authorized user when the authorized user requests access of the secured resource for a service client is a critical aspect of the present invention:

[8] We focus our analysis on claim 1. Claim 11 recites substantially the same limitations as a method. *Compare* Ex. 1001, claim 1, *with id.*, claim 11.

> *In a critical aspect* of the authentication system 30 and method 46 *of the present invention*, an additional security measure is implemented by requiring that the service client 33 be restricted from access to the common identifier for the secured resource, e.g. the account number for a credit card or financial deposit account; the Social Security Number of a patient; the account number of an ATM card; or the like.

Id. at 8:4–10 (emphasis added); *see also id.* at 10:29–36 ("*In accordance with a critical aspect of the present invention*, however, the automobile fueling station, restaurant or on-line retailer cannot be provided with or otherwise be made aware of either the consumer's credit card or checking account number and also must not be given any information that would allow the automobile fueling station, restaurant or on-line retailer to repeat the transaction without again obtaining authorization from the consumer." (emphasis added)). The '079 patent further emphasizes the importance of restricting the service client from having full access to the secured resource. *Id.* at 7:14–46.

Our reviewing court has found disavowal or disclaimer of claim scope based on clear and unmistakable statements by the patentee that limit the claims, such as "the present invention includes . . ." or "the present invention is . . ." or "all embodiments of the present invention are . . . ." *See*, *e.g.*, *Regents of Univ. of Minn. v. AGA Med. Corp.*, 717 F.3d 929, 936 (Fed. Cir. 2013); *Honeywell Int'l, Inc. v. ITT Indus., Inc.*, 452 F.3d 1312, 1316–19 (Fed. Cir. 2006); *SciMed*, 242 F.3d at 1343–44. Similarly, our reviewing court also has limited a claim element to a feature of the preferred embodiment when the specification described that feature as a "very important feature . . . in an aspect of the present invention," or as a "critical aspect of the present invention." *Inpro II Licensing, S.A.R.L. v. T-Mobile*

USA Inc., 450 F.3d 1350, 1354–55 (Fed. Cir. 2006); *Curtiss-Wright Flow Control Corp. v. Velan, Inc.*, 438 F.3d 1374, 1379–80 (Fed. Cir. 2006); *see also Andersen Corp. v. Fiber Composites, LLC*, 474 F.3d 1361, 1367–68 (Fed. Cir. 2007) (limiting the scope of all of the claims based on a "critical element" described in the specification); *Izumi Prods. Co. v. Koninklijke Philips Elecs. N.V.*, 140 F. App'x 236, 243–44 (Fed. Cir. 2005) (non-precedential) (limiting the scope of the claims based on the specification "defining a critical aspect of the invention itself").

Based on the '079 patent's discussion of the "critical aspect" of "the present invention," we are persuaded by Patent Owner's argument and further limit the "key string" in the server limitation (claim 1) and the determining step (claim 11) to one that does not reveal a common identifier of the secured resource to the service client. Notably, the '079 patent describes this need to prevent the discovery of a common identifier of the secured resource as the only "critical aspect" of "the present invention." According, we conclude that the patentee has disavowed or disclaimed claim scope based on clear and unmistakable statements describing the critical aspect of the present invention.

We are not persuaded by Petitioner's argument that because Patent Owner does not argue that Johnson does not teach the "key string" limitation, we do not need to address the proper construction of "key string." *See* Reply 4. First, the burden of persuasion to prove unpatentability is always on Petitioner and never shifts to Patent Owner. *In re Magnum Oil Tools Int'l, Ltd.*, 829 F.3d 1364, 1375 (Fed. Cir. 2016); *see also* 35 U.S.C. § 316(e). Similarly, the burden of production never switches from Petitioner

to Patent Owner with regard to the *Graham* factors, such as the differences between the scope of the claim and the prior art:

> Where, as here, the only question presented is whether due consideration of the four *Graham* factors renders a claim or claims obvious, no burden shifts from the patent challenger to the patentee. This is especially true where the only issues to be considered are what the prior art discloses, whether there would have been a motivation to combine the prior art, and whether that combination would render the patented claims obvious.

Magnum, 829 F.3d at 1376. Accordingly, whether or not Patent Owner argues a prior art reference does not teach a limitation, Petitioner retains the burden to prove that the prior art teaches or suggests all of the limitations recited in the claim. Moreover, in determining whether Petitioner has met that burden, it is proper for us to interpret the challenged claims based on the full record developed during trial, not based on how any terms were interpreted preliminarily in the Decision on Institution. *See Trivascular*, 812 F.3d at 1068 (holding that "the Board is considering the matter preliminarily without the benefit of a full record" at the institution stage, and "[t]he Board is free to change its view of the merits after further development of the record, and *should do so* if convinced its initial inclinations were wrong").

Second, contrary to Petitioner's argument, Patent Owner asserts that Johnson does not teach a "key string" under Patent Owner's proposed definition. For example, Patent Owner asserts that "Johnson does not show a single-payment transaction system like the '079 system which allows the buyer to authorize the merchant's access to the buyer's credit card account to pay for a given transaction without having to give any credit card details to the merchant." PO Resp. 36. Similarly, in summarizing its arguments, Patent Owner states Johnson does not teach or suggest, *inter alia*,

"determining a key string known to both said secured resource and the authorized user said requestor purports to be, said key string being adapted to provide a basis for authenticating the identity of said requester." *Id.* at 43 (emphasis omitted). The fact that Patent Owner does not include any further argument regarding that contention in the Patent Owner Response is immaterial, as we must determine whether Petitioner has met its burden to prove unpatentability by a preponderance of the evidence.

Petitioner further argues that Patent Owner's proposed construction "assumes that the claims require the 'key string' to be the same as the 'authentication credential.'" Reply 3. According to Petitioner, although "the '079 Patent specification discloses an embodiment where the 'authentication credential' can comprise a 'key string,' the claims are not so limited." *Id.*; *see also* Ex. 1017, 57:10–20, 61:3–11 (Mr. Oglesby opining that claim 1 is silent as to whether to not the key string and authentication credential are the same). We agree with Petitioner that the specific "key string" recited in the claim is not the same thing as the claimed "authentication credential." The claims recite both a "key string" and an "authentication credential" and no limitation recited in the claims requires that they must be—or even can be—the same thing. Because two different words are used, we are not persuaded that the limitations are synonymous. *See Ethicon Endo–Surgery, Inc. v. U.S. Surgical Corp.*, 93 F.3d 1572, 1579 (Fed. Cir. 1996) ("If the terms 'pusher assembly' and 'pusher bar' described a single element, one would expect the claim to consistently refer to this element as *either* a 'pusher bar' or a 'pusher assembly,' but not both, especially not within the same clause. Therefore, in our view, the plain

meaning of the claim will not bear a reading that 'pusher assembly' and 'pusher bar' are synonyms.").

However, our construction maintains a difference between the "key string" and the "authentication credential." As properly construed, the key string is used by the requester to request that a service client be able to have access to a secured resource. On the other hand, the authentication credential is used by the service client to access that secured resource. That is, although we have construed the "key string" such that it precludes systems and methods in which the key string, with its identifying information, is provided to the unauthorized service client, the "authentication credential" is given to the unauthorized service client to use for authentication. *Id*. at 17:37–43, 51–57. Because the "key string" cannot be known to the "unauthorized service client" and the "authentication credential" must be given to the "unauthorized service client," consistent with Petitioner's argument and Mr. Oglesby's testimony, the construction draws a distinction between the "key string" and the "authentication credential."[9]

As explained above, a "string" in the context of the '079 patent is "an ordered sequence of any subset of symbols selected from a set of symbols wherein each symbol forming the set may be represented in both a format that may be perceived by an end user and a format that may be recognized

[9] For clarity we note that although the authentication credential is not the key string recited in the server limitation (claim 1) or the determining step (claim 11), that is not to say that the authentication credential cannot have the attributes of a key string, except for the disclaimer. For example, the authentication credential may meet the definition of a "string" set forth in column 15 of the '079 patent.

by software or hardware." Ex. 1001, 15:29–36. Additionally, independent claims 1 and 11 further require that the "key string" be "known to both said secured resource and the authorized user said request[e]r purports to be" and "adapted to provide a basis for authenticating the identity of said requester." *Id*. at 17:40–42, 18:48–53. Moreover, based on the disclaimer explained above, we agree with Patent Owner and Mr. Oglesby that the claimed system and method must operate in a manner so that the "key string" does not reveal a common identifier of the secured resource to the unauthorized service client. *See* PO Resp. 26–28; Ex. 2004 ¶¶ 50–53. Stated differently, because the key string is adapted to provide a basis for authenticating the identity of the requester and providing access to the secured resource, the disclaimer acts to exclude systems and methods in which the key string, with its identifying information, is provided to the unauthorized service client. No further interpretation is necessary.

2. "Secured Resource" and "Input"

Having considered the evidence presented, in light of our findings regarding the key string limitation discussed below, we conclude that no express claim construction for "secured resource" and "input" is necessary for our determination. *See Vivid*, 200 F.3d at 803 ("[O]nly those terms need be construed that are in controversy, and only to the extent necessary to resolve the controversy.").

C. Legal Principles of Obviousness

An invention is not patentable "if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains."

35 U.S.C. § 103(a). The question of obviousness is resolved on the basis of underlying factual determinations including: (1) the scope and content of the prior art; (2) any differences between the claimed subject matter and the prior art; (3) the level of skill in the art; and, (4) where in evidence, objective evidence of nonobviousness, such as commercial success, long-felt but unsolved needs, and failure of others.[10] *Graham v. John Deere Co.*, 383 U.S. 1, 17–18 (1966). When evaluating a combination of teachings, we also must "determine whether there was an apparent reason to combine the known elements in the fashion claimed by the patent at issue." *KSR Int'l Co. v. Teleflex Inc.*, 550 U.S. 398, 418 (2007) (citing *In re Kahn*, 441, F.3d 977, 988 (Fed. Cir. 2006)). We analyze the grounds based on obviousness in accordance with the above-stated principles.

D. Level of Ordinary Skill in the Art

In determining the level of ordinary skill in the art, various factors may be considered, including the "type of problems encountered in the art; prior art solutions to those problems; rapidity with which innovations are made; sophistication of the technology; and educational level of active workers in the field." *In re GPAC, Inc.*, 57 F.3d 1573, 1579 (Fed. Cir. 1995) (citing *Custom Accessories, Inc. v. Jeffrey-Allan Indus., Inc.*, 807 F.2d 955, 962 (Fed. Cir. 1986)). In a given case, "one or more factors may predominate." *Id.*

[10] Neither Petitioner nor Patent Owner addresses objective evidence of non-obviousness. Accordingly, we do not address them in deciding whether or not Petitioner has met its burden to prove unpatentability.

In the Preliminary Response, Patent Owner asserted that a person having ordinary skill in the art at the time of the invention would have had the following level of skill:

> the equivalent of either a business degree (e.g., a bachelor's in business, economics, finance or similar discipline) or a degree in computing (e.g., a bachelor's in computer science, electrical engineering, or similar discipline), with at least two years of experience in designing and deploying electronic payment and security systems.

Prelim Resp. 20–21 (citing Ex. 2003 ¶ 41). Petitioner proposes a nearly identical level of ordinary skill in the art, differing only in the language—but not the substance—of the amount of experience. Pet. 12–13 (citing Ex. 1007 ¶ 60).

In the Decision, we adopted Patent Owner's definition of the level of ordinary skill in the art. Dec. 14. Neither Patent Owner nor Petitioner address the level of skill in their post-institution papers. Based on the complete record, we see no reason to modify our preliminary determination of the level of ordinary skill in the art.[11]

E. Obviousness over Johnson and Stambaugh

Petitioner asserts that the subject matter of claims 1, 6, 7, 9, 11, 16, 17, and 19 of the '079 patent would have been obvious to a person of ordinary skill in the art at the time of the invention in light of the teachings of Johnson and Stambaugh. Petitioner relies on Johnson (Ex. 1004), Stambaugh (Ex. 1005), and the Declaration of Stephen Craig Mott

[11] We note that our determination in this Final Written Decision would not change had we adopted Petitioner's proposed level of ordinary skill in the art.

(Ex. 1007). Based on the trial record, we are not persuaded that Petitioner has satisfied its burden of proving the claims are unpatentable.

1. Summary of Johnson

Johnson "relates to networked transaction systems and methods for conducting online transactions." Ex. 1004 ¶ 2. Johnson teaches, *inter alia*, a multi-party transaction protocol using "an end-user (purchaser) computer 110, a merchant computer 140, an identity provider computer 120, and a payment provider computer 130." *Id.* ¶ 46 (emphasis omitted). An annotated version of Figure 3 of Johnson provided by Petitioner (Pet. 19) is shown below:

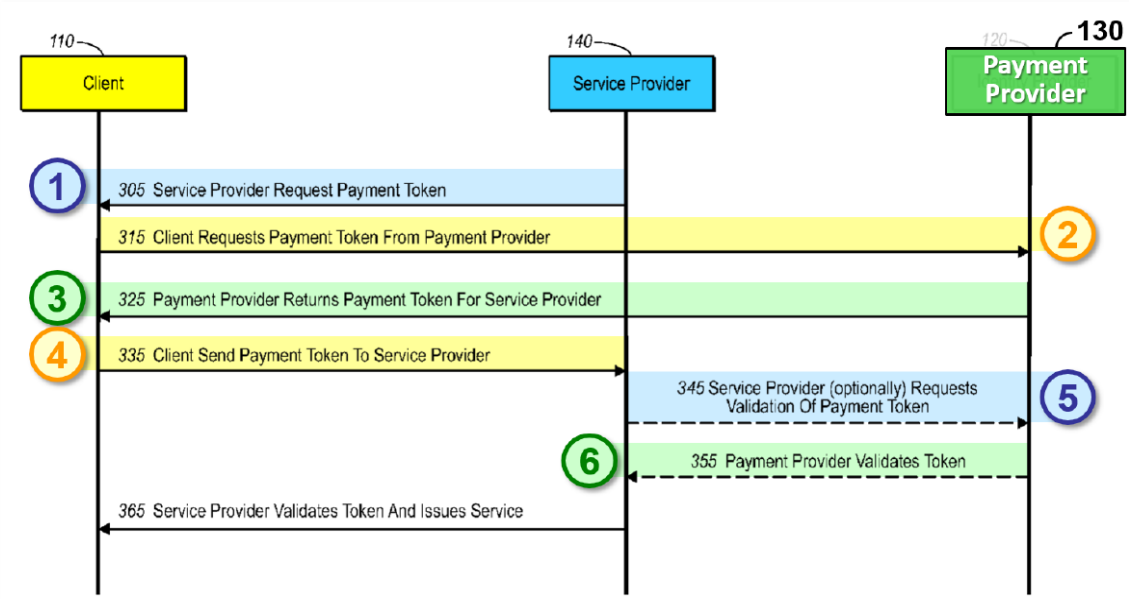

FIG. 3

Figure 3 "illustrates a diagram of a system and method for performing payment negotiation, verification and/or certification in an online transaction" which has been annotated by Petitioner to show what Petitioner

contends are the same six messaging steps[12] as shown in Figure 4 of the '079 patent. *See* Ex. 1004 ¶ 21; Pet. 17–20.[13]

First, a service provider requests a payment token from an end-user/client. Ex. 1004 ¶ 59, Fig. 3. Second, the end-user requests a payment token from a payment provider. *Id.* ¶ 60, Fig. 3. Third, once the payment provider has verified the identity of the end-user and the end-user's ability to pay, the payment provider "generate[s] and transmit[s] a payment token to the end-user computer." *Id.* ¶ 61, Fig. 3. Fourth, the end-user forwards the payment token to the service provider. *Id.* ¶ 61, Fig. 3. Fifth, the service provider requests the payment provider to validate the payment token. *Id.* ¶ 62, Fig. 3. Sixth, the payment provider sends a message back to the service provider indicating that the token is valid. *Id.* ¶ 62, Fig. 3.

2. Summary of Stambaugh

Stambaugh "relate[s] to using a wireless device, such as a cell phone, to pay for a transaction, and more particularly providing secure authentication for such payment transactions." Ex. 1005, 1:13–16. Stambaugh discloses a three-party transaction protocol between a user, a payment authority, and a merchant. *Id.* at 2:18–50. When a user wishes to purchase an item or service, the user uses a mobile device to send a message including a personal identification number (PIN) to the payment provider.

---

[12] Figure 3 also teaches a seventh step (step 365), which is not relevant to our analysis.

[13] In addition to the annotations, Petitioner changed the box labeled as "Identity Provider 120" to "Payment Provider 130," which we find is consistent with the disclosure of Johnson. *See* Pet. 19 n.1 (citing Ex. 1004 ¶ 59). Patent Owner does not address this change in its description of Johnson. *See* PO Resp. 13–14.

Id. at 2:18–37, 3:53–65, 6:25–33, 6:51–61, Fig. 4. The PIN is used to authenticate the user and, if authenticated, the payment provider sends the user a transaction code that can be used by the merchant to collect payment. *Id.* at 6:31–33, 6:41–44, 7:11–46, 7:59–61. In one embodiment, in addition to the transaction code, the user appends certain additional digits to the transaction code as an extra authentication factor. *Id.* at 8:19–30.

3. Claims 1, 6, 7, 9, 11, 16, 17, and 19

Petitioner relies on Johnson for many of the limitations of independent claims 1 and 11.[14] Pet. 24–55. For example, Petitioner contends Johnson teaches a payment provider/server having software "to determine a key string known to both said secured resource and the authorized user said requestor purports to be." *Id.* at 40–44.[15]

Having reviewed the record, we determine that Petitioner has not shown by a preponderance of the evidence that Johnson teaches or suggests a key string as recited in claims 1 and 11. Specifically, Petitioner maps Johnson's payment token to the key string recited in claims 1 and 11. *See* Pet. 41–44 (mapping the Johnson payment token to the recited "key string" limitation); Reply 4 (stating that Petitioner mapped the Johnson payment token to the recited "key string" limitation). The Johnson payment token is provided to the merchant. *E.g.*, Ex. 1004, Fig. 3 (payment token provided to

[14] System claim 1 and method claim 11 recite similar limitations. Petitioner relies on the evidence and arguments presented for claim 1 to show that the prior art teaches the various limitations of claim 11. Pet. 59–60.

[15] Because the "key string" limitation is case dispositive, we focus our analysis on that limitation, and need not address other limitations argued by Patent Owner in its Response.

client in step 325, payment token provided to service provider in step 335), ¶ 61 ("The end-user computer 110 may then forward the payment token to the merchant 140 (step 335)."). As discussed in the claim construction section above, *see supra* Section III.B.1, the disclaimer limits the system of claim 1 and the method of claim 11 to ones in which the key string, which is adapted to provide a basis for authenticating the identity of the requester (user/purchaser), does not reveal a common identifier of the secured resource to the unauthorized service client (merchant). Because the payment token is provided to the merchant/unauthorized service client in Johnson, the payment token does not satisfy all of the requirements of the "key string" limitation.

Petitioner also argues a person of ordinary skill in the art would have modified the Johnson payment token in light of the teachings of Stambaugh. *See* Pet. 44–48. Specifically, Petitioner contends that if the payment token taught by Johnson is not a key string because it is not viewable by a person, then Stambaugh teaches using a transaction number that is a variable length digit code, which is a "key string [that] may be both recognized by hardware/software and perceived by an end-user." *Id.* at 44–45. According to Petitioner, a person of ordinary skill in the art "would have readily appreciated that tokens, including specifically payment tokens, were most commonly ordered sequences of numbers and/or alphanumeric data" and "using an ordered sequence of numbers and/or alphanumeric data would have been the most natural and routine way . . . to implement Johnson's payment token." *Id.* at 45–46 (emphasis omitted) (citing Ex. 1007 ¶¶ 81–83). Additionally, Petitioner argues that a person of ordinary skill in the art

would have modified Johnson to use a code already known to the user and payment authority. *Id*. at 46–48.

However, even if a person of ordinary skill in the art modified the Johnson payment token in light of the teachings of Stambaugh, the modified token still would not have the characteristics required by the claimed "key string." Specifically, Petitioner does not argue that the payment token would no longer be given to the merchant/unauthorized service client or that the modification would result in a payment token that did not include a common identifier of the secured resource.

For the foregoing reasons, we determine Petitioner has not shown by a preponderance of the evidence that independent claims 1 and 11, or claims 6, 7, 9, 16, 17, and 19, which depend, directly or indirectly, from claims 1 or 11, are unpatentable over Johnson in view of Stambaugh. *See In re Fritch*, 972 F.2d 1260, 1266 (Fed. Cir. 1992) ("[D]ependent claims are nonobvious if the independent claims from which they depend are nonobvious.").

F. Obviousness over Johnson, Stambaugh, and Sellars

Petitioner asserts that the subject matter of dependent claims 3, 8, 13, and 18 of the '079 patent would have been obvious to a person or ordinary skill in the art at the time of the invention in light of the teachings of Johnson, Stambaugh, and Sellars. Petitioner relies on Johnson (Ex. 1004), Stambaugh (Ex. 1005), Sellars (Ex. 1006), and the Declaration of Stephen Craig Mott (Ex. 1007).

Petitioner does not rely on Sellars to remedy the deficiencies noted above with respect to the key string limitation recited in independent claims 1 and 11. *See* Pet. 64–72. Instead, Petitioner relies on Sellars as allegedly teaching determining the identity of a secured resource from amongst a

plurality of secured resources and generating a receipt. *Id*. As such, we determine Petitioner has not shown by a preponderance of the evidence that dependent claims 3, 8, 13 and 18 are unpatentable over Johnson in view of Stambaugh and Sellars. *See Fritch*, 972 F.2d at 1266 ("[D]ependent claims are nonobvious if the independent claims from which they depend are nonobvious.").

IV. CONCLUSION

We conclude that Petitioner has not demonstrated by a preponderance of the evidence that claims 1, 3, 6–9, 11, 13, and 16–19 of the '079 patent are unpatentable.

V. ORDER

In consideration of the foregoing, it is hereby:

ORDERED that claims 1, 3, 6–9, 11, 13, and 16–19 of the '079 patent are not determined to be unpatentable; and

FURTHER ORDERED that, because this is a Final Written Decision, parties to the proceeding seeking judicial review of the decision must comply with the notice and service requirements of 37 C.F.R. § 90.2.

IPR2017-00296
Patent 8,505,079 B2

PETITIONER:

Jason Mudd
Eric Buresh
ERISE IP, P.A.
jason.mudd@eriseip.com
eric.buresh@eriseip.com

Jonathan Stroud
Roshan Mansinghani
UNIFIED PATENTS INC.
jonathan@unifiedpatents.com
roshan@unifiedpatents.com

PATENT OWNER:

Sandeep Seth
SETH LAW OFFICES
ss@sethlaw.com

Andy Tindel
MANN, TINDEL & THOMPSON
atindel@andytindel.com